UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

CORPORATE RISK HOLDINGS LLC, *solely its capacity as the Plan Administrator Under the Amended Joint Chapter 11 Plan of Altegrity, Inc. et al.*,

Plaintiff,

-v-

SHARON T. ROWLANDS,

Defendant.

No. 17-cv-5225 (RJS)
ORDER AND MEMORANDUM

RICHARD J. SULLIVAN, District Judge:

Plaintiff Corporate Risk Holdings LLC ("CRH") brings this action against Defendant Sharon T. Rowlands, asserting claims for breach of fiduciary duty in connection with her alleged failures to monitor and oversee cybersecurity practices in her role as a director of United States Investigation Services ("USIS"), a subsidiary of Altegrity, Inc. ("Altegrity). (Doc. No. 26.) Now before the Court is Defendant Rowlands's motion to dismiss the Second Amended Complaint for failure to state a claim upon which relief can be granted. (Doc. No. 27.) For the reasons that follow, Defendant's motion is GRANTED.

I. BACKGROUND

A. Facts[1]

USIS, a subsidiary of Altegrity, provided background check services for the United States Office of Personnel Management (OPM) and various other federal agencies. (SAC ¶ 107.) It was

[1] The facts set forth below are taken from the Second Amended Complaint (Doc. No. 26 ("SAC")), statements or documents incorporated into the amended complaint by reference, and documents upon which Plaintiffs relied in bringing the suit. *See ATSI Commc'ns, Inc. v. Shaar Fund, Ltd.*, 493 F.3d 87, 98 (2d Cir. 2007). In ruling on the

originally formed in 1996 after Congress privatized a unit of OPM. (*Id.* ¶ 49.) In its role as a government contractor performing work outsourced from OPM, USIS conducted investigations regarding individuals employed by the federal government, individuals seeking employment with the federal government, and government contractors. (*Id.* ¶ 111.) In the course of its investigations, USIS collected individuals' education and employment histories, criminal backgrounds, credit records, and other sensitive information pertaining to applicants' personal lives, such as drug or gambling habits, extramarital affairs, psychiatric treatment, and the like. (*Id.* ¶ 112.) Rowlands was the Chief Executive Officer of Altegrity. (*Id.* ¶ 43.) She also served as a director on USIS's board of directors (the "Board"). (*Id.* ¶¶ 43, 44.)

The industry in which USIS operated was especially vulnerable to cyberattacks. After a string of high profile security incidents, government officials began to issue public warnings to government agencies, contractors, and private companies, urging them to take cybersecurity precautions to defend against such attacks. (*Id.* ¶ 115–18.) For example, at a public hearing in February 2012, NASA Inspector General Paul Martin indicated that NASA had experienced 47 attacks in the previous year, 13 of which successfully compromised NASA computer networks. (*Id.* ¶ 117.) Less than one month later, then–U.S. Defense Secretary Leon Panetta gave a speech at the University of Louisville in which he emphasized that cybersecurity threats posed a significant risk to the nation, and suggested that attacks were capable of bringing down entire power grids or disrupting national financial markets. (*Id.* ¶ 118.) Members of USIS leadership, including Rowlands, were aware of, and even publicly discussed, the threats posed by a potential cyberattack. (*Id.* ¶ 119.)

---

instant motion, the Court has also considered Defendant's memorandum of law in support of their motion to dismiss (Doc. No. 28 ("Mem.")), Plaintiff's opposition (Doc. No. 29 ("Opp'n")), Defendant's reply (Doc. No. 30 ("Reply")), Defendant's Notice of Supplemental Authority (Doc. No. 31), and Plaintiff's response (Doc. No. 33).

In response to such threats, OPM, USIS's largest client and revenue source, required USIS to meet certain minimum cybersecurity oversight requirements. (*Id.* ¶¶ 59, 60, 107–08.) To meet these requirements, USIS instituted cybersecurity measures that included network monitoring on weekdays and security logs keeping track of security issues such as failed login attempts, as well as various cybersecurity protocols that would be used to respond to cyberattacks. (*Id.* ¶¶ 2–3, 11, 16, 18, 22–31, 34, 59–60, 64, 67, 70–71, 80, 83, 121.) USIS also retained the IT services of Capgemini U.S. LLC, which managed, maintained, and assisted USIS in securing its cyber network, including the network that contained all of the confidential information acquired by USIS in the course of its work for the federal government. (*Id.* ¶ 74 & n.10.)

OPM found USIS's "compliance-driven" approach to cybersecurity sufficient to sustain USIS's "Authorization to Operate" ("ATO") (*id.* ¶¶ 64–67). This ATO certification was necessary for USIS to continue to conduct background checks on OPM's behalf (*id.* ¶¶ 92–94), and, furthermore, was a precondition for the renewal of the fieldwork and support contracts between OPM and USIS, which were set to expire on September 30, 2014 (*id.* ¶ 95). The contracts – worth $288 million and $2.46 billion, respectively – constituted a major source of revenue for both USIS and its parent company, Altegrity. (*Id.* ¶ 108.)

Despite the importance of cybersecurity to USIS's business, the Board did not have a dedicated subcommittee responsible for monitoring cybersecurity risk (*id.* ¶ 6), and the minutes taken at board meetings between February 12, 2012, and March 31, 2014 do not reference discussions of any cybersecurity oversight measures (*id.* ¶ 5). Indeed, it appears that during that period of time, no one formally reported to the Board on the status of USIS's own cybersecurity risks and vulnerabilities, or the precautions USIS was taking to address those threats. (*Id.* ¶ 143.)

No board member questioned any individual from USIS about whether additional safeguards should be implemented. (*Id.* ¶ 147.)

As it turned out, USIS's cybersecurity measures failed to protect USIS networks and data from breach and theft. According to the Second Amended Complaint, "malicious actors" first infiltrated USIS's systems on April 19, 2013. (*Id.* ¶ 17.) USIS's cybersecurity apparatus failed to detect this intrusion for a period of eight months, during which time the hostile actors conducted reconnaissance on USIS's internal networks. (*Id.* ¶ 18.) Then, on December 25, 2013, the hackers conducted a "brute force" attack using a trial and error hacking technique that allowed them to infiltrate the internal systems containing confidential information collected in the course of background check services. (*Id.* ¶¶ 19–21.) By the time USIS detected the intrusion – over six months later on June 5, 2014 – the hackers had stolen the confidential data of over 33,000 federal employees, potential employees, and contractors. (*Id.* ¶ 21.)

Upon detecting the intrusion, USIS immediately implemented a Computer Incident Response Plan and retained the services of a computer investigative firm to respond to and contain the ongoing breach. (*Id.* ¶¶ 70–71.) Nevertheless, two months later on August 6, 2014, OPM issued USIS a temporary "Stop-Work Order" and, on August 22, 2014, ultimately revoked USIS's ATO altogether. (*Id.* ¶¶ 88, 92). A contemporaneous report issued at the request of OPM by the U.S. Department of Homeland Security's Computer Emergency Readiness Team ("US-CERT") recommended that USIS overhaul its security apparatus in order to exceed, rather than simply meet, the minimum federal cybersecurity compliance requirements. (*Id.* ¶¶ 84, 89–91.)

On September 9, 2014, shortly after the release of US-CERT's report, OPM notified USIS that it would not renew USIS's fieldwork and support contracts, choosing instead to award those contracts to competitor firms. (*Id.* ¶¶ 95-96.) The loss of these contracts cost USIS approximately

$3 billion in revenue and eventually led both USIS and Altegrity to file for Chapter 11 bankruptcy on February 8, 2015. (*Id.* ¶¶ 97–99.)

B. Procedural History

Plaintiff commenced this action in New York state court on May 26, 2017, seeking to recover damages for breach of fiduciary duties under Delaware law.[2] (Doc. No. 1-1.) On July 17, 2017, the case was removed to this Court (Doc. No. 3) on diversity jurisdiction grounds, *see* 28 U.S.C. § 1332, and Plaintiff filed an Amended Complaint on August 11, 2017 (Doc. No. 12). Plaintiff filed a Second Amended Complaint on October 2, 2017 (Doc. No. 26), and Defendants filed a motion to dismiss on November 1, 2017 (Doc. No. 27), which was fully briefed on December 15, 2017 (Doc. No. 30). Defendant filed a memorandum of supplemental authority on December 28, 2017 (Doc. No. 31), to which Plaintiff responded on January 3, 2018. (Doc. No. 33.)

II. Legal Standard

To survive a motion to dismiss pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure, a complaint must "provide the grounds upon which [the] claim rests." *ATSI Commc'ns, Inc. v. Shaar Fund, Ltd.*, 493 F.3d 87, 98 (2d Cir. 2007); *see also* Fed. R. Civ. P. 8(a)(2) ("A pleading that states a claim for relief must contain . . . a short and plain statement of the claim showing that the pleader is entitled to relief . . . ."). To meet this standard, plaintiffs must allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

[2] CRH brings this action in its capacity as the Plan Administrator appointed under the Amended Joint Chapter 11 Plan of Altegrity, Inc. *et al.* (SAC at 4.)

In reviewing a Rule 12(b)(6) motion to dismiss, a court must accept as true all factual allegations in the complaint and draw all reasonable inferences in favor of the plaintiff. *ATSI Commc'ns*, 493 F.3d at 98. However, that tenet "is inapplicable to legal conclusions." *Iqbal*, 556 U.S. at 678. Thus, a pleading that offers only "labels and conclusions" or "a formulaic recitation of the elements of a cause of action will not do." *Twombly*, 550 U.S. at 555. If the plaintiff "ha[s] not nudged [its] claims across the line from conceivable to plausible, [its] complaint must be dismissed." *Id.* at 570.

III. Discussion

This case implicates the "failure-to-monitor" theory of director liability first articulated by the Delaware Court of Chancery in *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996). "*Caremark* claims inevitably arise in the midst of or directly following 'corporate trauma' of some sort or another," and are premised on directors' conscious failure to monitor corporate action, thereby "breaching their fiduciary duties in bad faith in a manner that caused the corporate trauma." *Horman v. Abney*, C.A. No. 12290-VCS, 2017 WL 242571, at *5 (Del. Ch. Jan. 19, 2017). Here, Plaintiff alleges that Rowlands breached her *Caremark* duties by failing to monitor USIS's cybersecurity practices despite the known risk of a cyberattack. This dereliction, according to Plaintiff, permitted a massive cyber-intrusion to go undetected for months, and eventually led to USIS's bankruptcy after its largest client revoked multi-billion dollar contracts in response to the security breach.

Plaintiff's theory of director liability has been repeatedly characterized as "possibly the most difficult theory in corporate law upon which a plaintiff might hope to win a judgment." *Caremark*, 698 A.2d at 967; *see also Stone ex rel. AmSouth Bancorporation v. Ritter*, 911 A.2d 362, 372 (Del. 2006); *In re Gen. Motors Co. Derivative Litig.*, C.A. No. 9627-VCG, 2015 WL 3958724, at *14 (Del. Ch. June 26, 2015), *aff'd*, 133 A.3d 971 (Del. 2016). That is because

Caremark liability is rooted in bad-faith conduct, not merely negligence. *Stone*, 911 A.2d at 369 ("[T]he Caremark standard for so-called 'oversight' liability draws heavily upon the concept of director failure to act in good faith."); *In re Citigroup Inc. S'holder Derivative Litig.*, 964 A.2d 106, 123 (Del. Ch. 2009) ("[A] showing of bad faith is a *necessary condition* to director oversight liability."); *City of Birmingham Ret. and Relief Sys. v. Good*, 177 A.3d 47, 55 (Del. 2017).

Consistent with the bad-faith requirement, a plaintiff must show more than a bad outcome or poor management. As Vice Chancellor Glasscock has observed, "[p]leadings, even specific pleadings, indicating that directors did a poor job of overseeing risk in a poorly-managed corporation do not imply director bad faith." *In re Gen. Motors Co. Derivative Litig.*, 2015 WL 3958724, at *17. Instead, there must be allegations suggesting bad faith approximating an "intentional dereliction of duty," *In re Walt Disney Co. Derivative Litig.*, 906 A.2d 27, 62 (Del. 2006), a "conscious disregard" for responsibilities, or actions taken "with intent to violate applicable positive law," *In re Citigroup*, 964 A.2d at 123. *See also Birmingham*, 177 A.3d at 55 (requiring that the defendant director "acted inconsistent with his fiduciary duties and, most importantly, that [he] *knew* he was so acting"); *Desimone v. Barrows*, 924 A.2d 908, 940 (Del. Ch. 2007) (requiring that complaint allege "the existence of facts suggesting that the board knew that internal controls were inadequate, that the inadequacies could leave room for illegal or materially harmful behavior, and that the board chose to do nothing about the control deficiencies that it knew existed").

Given this high burden, courts have viewed with skepticism claims premised on failure to monitor "business risk" or "exposure" to certain industry-wide risks. *See In re Citigroup*, 964 A.2d at 125. In the "typical" *Caremark* case, plaintiffs seek to hold directors liable "for damages that arise from a failure to properly monitor or oversee employee *misconduct* or *violations of law*."

In re Citigroup, 964 A.2d at 123 (emphasis added). That is because "[g]ood faith, not a good result, is what is required of the board." *Reiter ex rel. Capital One Fin. Corp. v. Fairbank*, C.A. No. 11693-CB, 2016 WL 6081823, at *14 (Del. Ch. Oct. 18, 2016) (quoting *In re Goldman Sachs Grp., Inc. S'holder Litig.*, C.A. No. 5215-VCG, 2011 WL 4826104 (Del. Ch. Oct. 12, 2011)). But as courts recognize, "there is a vast difference between an inadequate or flawed effort to carry out fiduciary duties and a conscious disregard for those duties." *Id.* (quoting *Lyondell Chem. Co. v. Ryan*, 970 A.2d 235, 243 (Del. 2009)).

Caremark's bad-faith theory of liability has been refined in later cases. When the Delaware Supreme Court formally adopted the "failure-to-monitor" theory originally developed in *Caremark*, the Court described two scenarios where a claim might be viable, the first involving situations in which directors utterly failed to implement any reporting or information system or controls at all, and the second limited to instances when directors, having implemented such a system or control, consciously failed to monitor or oversee its operations, thus "disabling themselves from being informed of risks or problems requiring their attention." *Stone*, 911 A.2d at 370. Applying that standard in this case, Plaintiff first argues that Rowlands utterly failed to implement any reporting or information system or controls *whatsoever*. In the alternative, Plaintiff argues that even if USIS formally had a cybersecurity monitoring system in place, Rowlands consciously failed to oversee that system, thereby permitting the massive security breach. The Court will address each argument in turn.

To begin with, Plaintiff complains that USIS "lack[ed] sufficient controls and failed to properly monitor its network for malicious traffic or activity." (SAC ¶ 29; *see, e.g.*, *id.* ¶¶ 16, 18, 22–31, 34, 59–60, 64, 67, 80, 83.) But in doing so, Plaintiff concedes that the USIS Board maintained "reporting or information systems or controls" as required by *Caremark* and its

progeny. (*Id.* ¶ 29.) By Plaintiff's own characterization, USIS's cybersecurity controls – deficient as they might have been in hindsight – included "limited network coverage from Monday through Friday, from 7:00 a.m. to 4 p.m." (*Id.*) This network coverage was comprised of IT security personnel, network monitoring and security logs, and various other cybersecurity protocols. (*Id.* ¶¶ 2–3, 11, 16, 18, 22-31, 34, 59–60, 64, 67, 70–71, 80, 83.) Moreover, USIS retained the IT services of Capgemini U.S., LLC, which managed, maintained, and assisted USIS in securing its cyber network. (*Id.* ¶ 74 & n.10.) In fact, OPM itself agreed that USIS had at least *some* precautions in place when it certified that USIS had complied with its minimum cybersecurity requirements for federal contractors. (*Id.* ¶¶ 59–60.) Indeed, upon detecting the security breach, USIS quickly moved to address the breach with contingency plans to ascertain and mitigate the harm – showing, at the very least, that USIS had a reporting system in place. (*Id.* ¶¶ 70, 82.) No more is required to foreclose liability under this first category of *Caremark* liability. *See Cent. Laborers' Pension Fund v. Dimon*, 638 F. App'x 34, 38 (2d Cir. 2016); *see also David B. Shaev Profit Sharing Account v. Armstrong*, No. CIV.A. 1449-N, 2006 WL 391931, at*5 (Del. Ch. Feb. 13, 2006), *aff'd*, 911 A.2d 802 (Del. 2006) (holding that *Caremark* claims did not arise because plaintiff conceded defendant had compliance systems in place).

Taking a different tack, Plaintiff attempts to sidestep the obvious existence of cybersecurity controls at USIS by claiming that the relevant "system" USIS lacked was really the "system" of reporting breaches to the Board, not the cybersecurity measures in place. To bolster this argument, Plaintiff alleges that Rowlands and the Board failed to institute a subcommittee specifically responsible for cybersecurity monitoring and, apparently, had no discussions about cybersecurity at board meetings. (SAC ¶¶ 6, 14 (citing board minutes).)

But the Board's alleged failure to explicitly address cybersecurity at its meetings is insufficient to establish that the Board utterly failed to implement any information or reporting system or controls whatsoever. *See, e.g.*, *In re Gen. Motors Co. Derivative Litig.*, 2015 WL 3958724, at *14 ("Contentions that the Board did not receive specific types of information do not establish that the Board utterly failed 'to attempt to assure a reasonable information and reporting system exists'" (citation omitted)); *Horman v. Abney*, 2017 WL 242571, at *9 (rejecting plaintiffs' argument that the board's "deafening silence" on this relevant issue evinced a conscious disregard of its duties or a lack of oversight). It is a fundamental axiom of corporate governance that boards are not presumed to be involved in every conceivable act of corporate management. The fact remains that USIS's cybersecurity information systems and controls eventually detected the 2013-2014 intrusion (SAC ¶ 70), and, in response to that intrusion, USIS immediately implemented its "Computer Incident Response Plan" to halt further harm from arising. (SAC ¶ 70; Mem. at 6–7.) *Caremark* requires only that a reporting system exist, not even that it be "reasonable." *See Central Laborers' Pension Fund v. Dimon*, 638 F. App'x 34, 37–38 (2d Cir. 2016) (observing that the *Caremark* "standard's plain language could not be any clearer – 'any' simply does not mean 'reasonable'"). Clearly, the absence of board minutes falls short of establishing that the directors "knew they were not discharging their fiduciary obligations" to create a reporting system, or that they had a "conscious disregard" for that responsibility. *In re Citigroup*, 964 A.2d at 123. Therefore, Plaintiff has not established *Caremark* liability on the basis that no reporting system was in place.

Turning to the second half of the *Caremark* standard, Plaintiff alternatively argues that Defendants consciously failed to oversee any system that might have been in place, thereby permitting the massive security breach. *See, e.g.*, *Stone* 911 A.2d at 370; *see also In re Citigroup*,

964 A.2d at 123. Plaintiff again faces a high hurdle, since simply alleging that a bad outcome occurred is not sufficient to state a claim under *Caremark*. Here, to establish the requisite scienter, a plaintiff may rely on the existence of so-called "red flags" – "evidence of corporate misconduct" – that directors knowingly ignored, thereby rendering existing control systems powerless to prevent harmful or illegal conduct. *See Reiter*, 2016 WL 6081823, at *8. However, warning signs concerning business risk – that is, a company's escalating exposure to risk in light of business decisions or broader industry trends – are insufficient, by themselves, to meet this standard. *Id* at 13; *see also In re Citigroup*, 964 A.2d at 123 (characterizing plaintiffs' unsuccessful claims as "based on defendants' alleged failure to properly monitor [the company's] *business risk*"). Put another way, although the Board must respond to red flags pointing to an actual compliance failure or instance of corporate misconduct, no such "duty to respond" exists for "yellow flags" concerning business risk. *See Reiter*, 2016 WL 6081823, at *13. Such a distinction is entirely sensible given *Caremark*'s emphasis on bad faith, and courts have uniformly enforced it in *Caremark* cases.

Here, Plaintiff's case amounts to an allegation that the Board knew about the risk posed by a cyberattack, but did not adequately monitor USIS's cybersecurity efforts. But like the plaintiffs in *In re Citigroup Inc. Shareholder Derivative Litigation*, Plaintiff's focus on a specific, industry-wide risk is not sufficient to support a *Caremark* claim. *See* 964 A.2d at 128. In *Citigroup*, shareholders brought a derivative suit against Citigroup's officers and directors alleging that they breached their fiduciary duties by failing to adequately protect Citigroup from exposure to risks associated with the subprime lending market, ultimately resulting in massive financial losses for the bank. *Id*. at 112. The shareholders cited risk factors they believed the directors should have paid more attention to, which the Delaware Court of Chancery characterized as "statements from

public documents that reflect[ed] worsening conditions in the financial markets, including the subprime and credit markets, and the effects those worsening conditions had on market participants, including Citigroup's peers." *Id.* at 114–15. The Delaware Court of Chancery nevertheless rejected the plaintiffs' efforts to turn "bad business decisions" into evidence that the directors "consciously disregarded their duties or otherwise acted in bad faith." *Id.* at 128. In fact, the court found that it was irrelevant that the directors might have known of "signs of a deterioration in the subprime mortgage market" or "signs suggesting that conditions could decline further;" their knowledge of the significant risk posed by subprime lending was *still* insufficient "to show that the directors were or should have been aware of any wrongdoing at [Citigroup] or were consciously disregarding a duty to somehow prevent Citigroup from suffering losses." *Id.*

Plaintiff here uses the same tactics as the *Citigroup* plaintiffs in an attempt to re-cast the general and well-publicized business risk posed by a cyberattack into a "red flag" that sustains a *Caremark* claim of individual director liability. But the "red flags" cited by Plaintiff are nothing more than industry-wide generalizations about cybersecurity risks, not company-specific evidence of misconduct or compliance failure necessary to sustain a claim for director liability. For instance, Plaintiff's "red flags" include:

- A Lloyd's of London's Risk Index that identified "cybersecurity" as the "second-highest perceived risk for business leaders in the U.S. and Canada" (SAC ¶ 103);

- A June 2014 speech by then–Securities and Exchange Commission Commissioner Luis Aguilar – given months *after* the initial intrusion into USIS's system – in which the Commissioner cautioned, among other things, that "[e]nsuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director[s'] risk oversight responsibilities" (*id.* ¶ 104);

- An article published in July 2016 by American International Group, Inc. – *years* after the cyberattack at the center of this litigation – stressing that although "day-to-day responsibility for cybersecurity may lie with senior management and IT personnel," the "rapid escalation in cyberattack threats" necessitated "board-level" attention (*id.* ¶ 105); and

- A string of publicized attacks against government agencies and contractors in the years 2003 to 2018 (*id.* ¶¶ 115–18).

Plaintiff also focuses on the importance of data security to USIS's business, the dire consequences of any data breach, and the obviousness of the risk. Plaintiff stresses that "Defendant Rowlands herself warned of the growing threat of cyberattacks and cautioned companies like USIS to take a proactive approach to cybersecurity." (*Id.* ¶ 119.)

Because none of these self-styled "red flags" are "evidence of corporate misconduct," Plaintiff's theory would require the Court to expand director liability under *Caremark*, a point that Plaintiff itself concedes by expressly asking the Court to apply a new standard in light of the "unique nature" of a cyberattack. (Opp'n at 20.) But Plaintiff's justification for doing so rests upon the unpersuasive claim that cyberattacks, unlike "traditional illegal conduct," are "covert" and "not readily apparent," such that "there will rarely, if ever, be red flags of an attack *before* it takes place." (Opp'n at 20, 4.) Plaintiff fails to offer any explanation or legal basis for why cyberattacks are any more or less intrinsically covert than other kinds of illegal or harmful conduct contemplated by *Caremark*. There is simply no reason for the Court to alter the definition of "red flag," and indeed, the Court is not free to expand the Delaware courts' articulation of that standard.

At bottom, this case presents "a classic example of the difference between allegations of a breach of the duty of care (involving gross negligence) as opposed to the duty of loyalty (involving allegations of bad-faith conscious disregard of fiduciary duties)." *In re Gen. Motors Co. Derivative Litig.*, 2015 WL 3958724, at *17. Plaintiff's complaint amounts to nothing more than an attempt to impose personal liability upon a director for business decisions that turned out poorly for USIS. But none of the "red flags" alleged by Plaintiff point to bad faith misconduct. Rather, Plaintiff has identified, at most, a growing industry-wide awareness of cybersecurity threats

coupled with the USIS Board's decision to allocate a certain amount of resources to cybersecurity efforts. Thus, while Plaintiff may be correct that the Board mismanaged business risk by declining to invest additional company resources in a more robust cybersecurity system, such a claim does not satisfy the "exacting" standard for liability under *Caremark* – a standard that becomes yet more exacting "when, as here, the claims involve a failure to monitor *business* risk, as opposed to legal risk." *Wayne Cty. Emp.'s Ret. Sys. v. Dimon*, 629 F. App'x 14, 15 (2d Cir. 2015).

IV. CONCLUSION

For the reasons stated above, Plaintiff's attempt to convert bad monitoring and a bad outcome into bad faith fails, since the conduct alleged in the Second Amended Complaint falls far short of the high bar required to find liability under either prong of *Caremark*. Accordingly, Defendant's motion to dismiss is GRANTED. The Clerk of Court is respectfully directed to terminate the motion pending at docket number 27 and to close this case.

SO ORDERED.

Dated: September 28, 2018
New York, New York

RICHARD J. SULLIVAN
UNITED STATES DISTRICT JUDGE